JS Bank Limited

Wholesale Branch, Kingdom of Bahrain
(Licensed as Conventional Wholesale Bank (Branch) by CBB)

Online Security

Your security is our top priority. Please follow these guidelines to protect your online banking access and transactions:

1. Secure Access to the Portal

- Always access the online banking portal by typing our official website address into your browser. Do not use links from emails, SMS, or other messages.
- After each session, log out completely. Simply closing the browser is not enough.
- Use a strong and unique password. Update it regularly and avoid reusing it across other websites.

2. Two-Factor Authentication (2FA)

- Our portal uses **Microsoft Authenticator** and **Google Authenticator** for enhanced protection.
- Never share your one-time codes with anyone. The bank will never request these from you.

3. Secure Devices and Networks

- Use only trusted devices and secure networks. Avoid public Wi-Fi or shared computers.
- If connecting remotely, use a secure VPN.
- Keep your devices, operating systems, and browsers updated with the latest security patches and versions.

4. Monitor Your Accounts

- Regularly review your statements and transaction history.
- If you notice suspicious activity, contact us immediately using our official contact details.
- Monitor email alerts to stay informed about account activity in real time.

5. Keep Your Contact Information Updated

- Ensure your registered **mobile number and email** are up to date so you can receive security alerts and transaction confirmations promptly.

6. Beware of Phishing and Fraud Attempts

- Do not click links or open attachments in unexpected emails, SMS, or instant messages.
- Be cautious of callers or messages creating urgency and requesting passwords, codes, or personal details.
- Always type the bank’s official web address directly and look for “https://” in the address bar.

7. Protect Your Devices from Malware

- Install and update antivirus or anti-malware software.
- Do not store banking credentials in browsers or enable auto-fill.
- Keep devices locked when unattended and never share them with unauthorized persons.

8. Privacy and Terms

- Review our **Privacy Notice** to understand how your data is collected, shared, and protected.
- Familiarize yourself with the **Terms and Conditions of Online Banking** before using the service.

9. Stay Informed

- Cybersecurity risks evolve constantly. Stay alert to new threats and best practices.

We will share security reminders through our official channels.